UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

ALBERTA STEWART, on behalf of herself and all others similarly situated, Plaintiff, v. GREENSBORO COLLEGE, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Alberta Stewart ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following against the above-captioned Defendant Greensboro College, Inc. ("Defendant" or "Greensboro") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach"). On information and belief, the Data Breach has impacted at least 52,569 individuals.

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, Social Security numbers, address, financial account number, and credit and/or debit card numbers in combination

with security code, access code, password or PIN for the account ("personally identifying information" or "PII").

3. Greensboro's breach differs from typical data breaches because it affects at least some consumers who had no relationship with Greensboro, never sought one, and never consented to Greensboro collecting and storing their information.

4. On information and belief, the Data Breach occurred on August 10, 2023. However, Greensboro did not become aware of suspicious activity on its network until August 17, 2023, and cybercriminals had unfettered access to its network system until August 21, 2023.

5. Greensboro struggled to identify what information and which individuals were impacted by the Data Breach and took until February 5, 2024, to complete their internal investigation.

6. On February 29, 2024, Greensboro finally began notifying Class Members about the widespread Data Breach ("Notice Letter"). The Notice Letter Plaintiff received is attached as Exhibit A.

7. Greensboro waited over six months before finally informing Class Members of the Breach, even though Plaintiff and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. Greensboro's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how the breach happened or why

Greensboro delayed notifying victims that hackers had gained access to highly sensitive PII.

9. Defendant's failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

10. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

11. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed 52,569 individuals.

12. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff Alberta Stewart is a Data Breach victim.

14. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

15. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, consumers' private information was exactly that—private. Not anymore. Now, consumers' private information is forever exposed and unsecure.

PARTIES

16. Plaintiff, Alberta Stewart, is a natural person and citizen of North Carolina, where she intends to remain. Plaintiff is a Data Breach victim, receiving the Breach Notice on March 14, 2024.

17. Defendant, Greensboro College, Inc. of North Carolina, is a North Carolina Non-Profit Corporation, with its principal place of business at 815 W. Market Street, Greensboro, North Carolina 27401-1875.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class.

19. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

Greensboro College

21. Greensboro College is a private liberal arts college located in Greensboro, North Carolina. Founded in 1838, Greensboro "provides a coeducational and independent learning atmosphere with approximately 1,000 undergraduate students." Greensboro College employs 45 full-time faculty who teach 38 majors and more than 1,000 different courses.[1] Greensboro College boasts an annual revenue of $26.8 million.[2]

22. On information and belief, Greensboro accumulates highly sensitive PII of its consumers.

23. In collecting and maintaining its consumers' PII, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

24. Indeed, Greensboro boasts in its privacy policy that it "recognizes our obligations to keep your information secure and confidential."[3]

25. In collecting and maintaining consumers' PII, Greensboro agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

---

[1] About, Greensboro College, https://www.greensboro.edu/about/history-mission-vision/ (last visited March 19, 2024).
[2] Greensboro College Inc, ProPublica, https://projects.propublica.org/nonprofits/organizations/560532144 (last visited March 19, 2024).
[3] Privacy Policy, Greensboro College, https://www.greensboro.edu/privacy-policy/ (last visited March 19, 2024).

26. Despite recognizing its duty to do so, on information and belief, Greensboro has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' sensitive PII or supervised its IT or data security agents and consumers to prevent, detect, and stop breaches of its systems. As a result, Greensboro leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

27. Plaintiff is not affiliated with Greensboro College and is unsure how Greensboro got her information.

28. On information and belief, Greensboro collects and maintains former and current students', applicants, and consumers' unencrypted PII in its computer systems.

29. In collecting and maintaining the PII, Greensboro implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

30. According to the Breach Notice, "[o]n August 17, 2023, Greensboro College discovered suspicious activity related to some of its computer systems". Following an internal investigation, Greensboro discovered that "certain computer systems were subject to unauthorized access between August 10, 2023 and August 21, 2023." Ex. A.

31. In other words, Greensboro's investigation revealed that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its former and current consumers' highly sensitive PII.

32. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

33. On or around February 29, 2024 –more than six months after the Breach first occurred – Greensboro finally notified Plaintiff and Class Members about the Data Breach.

34. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing consumers' PII, as evidenced by the Data Breach.

35. In response to the Data Breach, Defendant contends that it has or will be "instituting additional technical safeguards and policies and procedures." Ex. A. Although Defendant fails to expand on what these alleged "additional technical safeguards" are, such steps should have been in place before the Data Breach.

36. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring your free credit reports for suspicious activity and to detect errors." Ex. A.

37. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

38. On information and belief, Greensboro has offered 24 months of complimentary credit monitoring services to victims, which does not adequately address

the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

39. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Because of the Data Breach, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiff and the Class Members with relief for the damages they suffered and will suffer.

41. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the infrastructure and manufacturing adjacent industries preceding the date of the breach.[4]

[4] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited March 19, 2024); *See also* Cost of a Data Breach: Infrastructure, security Intelligencehttps://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited March 19, 2024).

43. In light of recent high profile data breaches at other manufacturing and infrastructure companies, Defendant knew or should have known that its consumers' PII would be targeted by cybercriminals.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

45. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [7]

---

[5] 2021 Data Breach Annual Report, ITRC, https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited March 19, 2024).

[6] *Id*.

[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 19, 2024).

46. In 2023, manufacturing and infrastructure adjacent industries were warned to be one of the most-breached sectors[8] and cost, on average, $4.82 million per breach.[9]

47. Cyberattacks on infrastructure companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report cautioned, "Cyber risk in the financial system has grown over time as the system has become more digitized, as evidenced by the increase in cyber incidents."[10]

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Greensboro.

Plaintiff's Experience

49. Plaintiff Stewart received Greensboro's Breach Notice in or around March 2024.

50. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over six months.

---

[8] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited March 19, 2024).

[9] Cost of a Data Breach: Infrastructure, security Intelligence, https://securityintelligence.com/articles/cost-data-breach-infrastructure/ (last visited March 19, 2024).

[10] Implications of Cyber Risk for Financial Stability, Federal Reserve, https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited March 19, 2024).

51. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

52. Plaintiff does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

53. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

54. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

55. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

57. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

58. Indeed, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls, up to a dozen a day, suggesting that her PII is now in the hands of cybercriminals.

59. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[9] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

60. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

61. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

62. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

63. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

64. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

65. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

66. One such example of criminals using PII for profit is the development of "Fullz" packages.

67. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

68. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

69. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity including theft and sale on the dark web. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

70. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

71. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

73. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

74. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

76. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

77. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

78. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees

can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

79. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

80. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

81. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

82. Plaintiff sues on behalf of herself and the proposed class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> All individuals residing in the United States whose PII was compromised in the Greensboro Data Breach including all those who received notice of the breach.

83. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

84. Plaintiff reserves the right to amend the class definition.

85. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is a representative of the Class consisting of 52,569 members, far too many to join in a single action.

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control.

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests,

and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

86. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

87. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

88. Plaintiff and members of the Class entrusted their PII to Greensboro. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

89. Greensboro was under a basic duty to act with reasonable care when it undertook to collect, create, maintain, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the

prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

90. Defendant knew that the PII of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harm that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

91. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

92. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff' and the other Class member's PII.

93. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by

unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

94. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew its systems and technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

95. As a result of this misconduct by Defendant, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

96. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

97. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

99. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

100. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

101. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

102. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

103. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

104. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

105. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

106. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

107. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Greensboro fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Violation Of North Carolina Unfair Trade Practices Act
(On Behalf of Plaintiff and the Class)

108. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

109. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

110. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

e. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

111. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

112. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

113. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

114. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff's and Class members' rights.

115. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

116. Defendant's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

117. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

COUNT IV
Breach Of Contract
(On Behalf of Plaintiff and the Class)

118. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

119. Defendant entered into various contracts with its clients, to provide services to its clients.

120. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that

Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

121. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

122. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

123. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

124. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

125. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

126. Plaintiff and Class Members conferred a benefit upon Defendant in providing their PII to Defendant.

127. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members. And Defendant benefited from receiving Plaintiff's and Class Members' PII, as this was used to facilitate its business.

128. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

129. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

130. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' services because Defendant failed to adequately protect their PII.

131. Plaintiff and Class Members have no adequate remedy at law.

132. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: March 21, 2024

Respectfully submitted,

/s/ Scott C. Harris

Scott C. Harris (SBN 35328)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan Street
Raleigh, NC 27603
Telephone: (919) 600-5003
sharris@milberg.com

Samuel J. Strauss *
sam@turkestrauss.com
Raina C. Borrelli *
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

**Pro Hac Vice Application forthcoming*

Attorneys for Plaintiff and the proposed Class